UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA
WILKES-BARRE DIVISION

TATIANA ADKINS individually, and on behalf of all others similarly situated, Plaintiff, v. MATERNAL & FAMILY HEALTH SERVICES, INC., Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Tatiana Adkins ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Maternal & Family Health Services, Inc., ("MFHS" or "Defendant"), by and through her attorneys, and allege, based upon personal knowledge as to her own actions and her counsels' investigation, and based upon information and belief as to all other matters, as follows:

INTRODUCTION

1. MFHS is a private, health and human services organization operating in Northeastern Pennsylvania. It provides health and nutrition needs services through a network of health and nutrition centers in 17 Pennsylvania Counties serving more than 90,000 women, men, and children through core programs of WIC (women, infants and children) Nutrition, Reproductive Health, Nurse-Family Partnership and Pregnancy Care. MFHS is headquartered in Wilkes-Barre Pennsylvania.[1]

[1] *About Us*, Maternal & Family Health Services, https://www.mfhs.org/about-us/ (last accessed February 23, 2023).

2. As a health and nutrition center providing a wide variety of medical services and nutritional services, MFHS collects, maintains, and stores its patients' highly sensitive personal and medical information including, but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, driver's license numbers, information regarding medical treatment, diagnosis, and prescriptions, medical record numbers, health insurance information, other protected health information ("personally identifying information" or "PII") and financial account/payment card information.[2]

3. Although MFHS is a sophisticated medical entity providing services to hundreds of thousands of patients, MFHS failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and medical information of approximately 461,070 individuals, including the Plaintiff and Class members.[3] As a direct, proximate, and foreseeable result of MFHS's failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised MFHS's network and accessed 461,070 of patient files containing highly-sensitive PII.[4]

4. Specifically, sometime in or around August 21, 2021, MFHS's patients' sensitive personal and medical data was compromised when unauthorized actors were able to successfully launch a ransomware attack, which resulted a breach MFHS's network and access files containing approximately 461,070 individual's PII (the "Data Breach").[5]

---

[2] *Important Information about Maternal & Family Health Services' 2022 Cybersecurity Incident,* https://www.mfhs.org/important-information-about-maternal-family-health-services-2022-cybersecurity-incident/(last accessed February 23, 2023).
[3] *See Data Breach Notification*, Office of Maine Atty. General, https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml. (last visited February 22, 2023).
[4] *Id.*
[5] *Id.*

5. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers and medical information, are extremely sensitive and are known to be highly valuable to thieves, MFHS failed to detect the breach until on or around April 4, 2022—more than **eight months** after unauthorized individuals accessed Plaintiff's and current and former patients' highly sensitive PII stored on MFHS's systems.

6. MFHS's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to MFHS's security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

7. MFHS failed to take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former patients the material fact that it lacked appropriate data systems and security practices to secure PII and medical information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to MFHS's failures, Plaintiff and approximately 461,070 individuals suffered substantial harm and injury.

8. As a result of MFHS's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of MFHS's current and former patients. Plaintiff and Class

members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors.

9. Plaintiff and Class members suffered injuries as a result of MFHS's conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in MFHS's possession and is subject to further unauthorized disclosures so long as MFHS fails to undertake appropriate and adequate measures to protect their PII. These risks will remain for the lifetimes of Plaintiff and the Class.

10. Accordingly, Plaintiff bring this action on behalf of all those similarly situated to seek relief from MFHS's failure to reasonably safeguard Plaintiff's and Class members' PII; its failure to reasonably provide timely notification that Plaintiff's and Class members' PII had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII.

PARTIES

Plaintiff Tatianna Atkins

11. Plaintiff Tatianna Atkins is a resident and citizen of Pennsylvania, residing in Hanover Township, Pennsylvania. Plaintiff Atkins is a former patient of MFHS. Plaintiff Atkins received a data breach letter from Defendant dated January 10, 2023.

Defendant Maternal Health & Family Services

12. Defendant Maternal Health & Family Services is a health and human services non-profit corporation incorporated under the laws of the State of Pennsylvania, with its principal place of business at 15 Public Square, Suite 600, Wilkes-Barre, PA 18701.

JURISDICTION AND VENUE

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has personal jurisdiction over Defendant because Defendant is authorized to and regularly conducts business in Pennsylvania, and is headquartered in Wilkes-Barre, Pennsylvania.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Maternal & Family Health Services - Background

16. MFHS provides health and nutrition needs services through a network of health and nutrition centers in 17 Pennsylvania Counties serving more than 90,000 women, men, and children through core programs of WIC (women, infants and children) Nutrition, Reproductive Health, Nurse-Family Partnership and Pregnancy Care.[6] MFHS represents to its patients that it "meets the ever-changing needs of women, children, and families by providing essential and innovative programming that improves the quality of life for women, children, and families."[7]

17. As part of their medical and business operations, MFHS collects, maintains, and stores the highly sensitive PII and medical information provided by its current and former patients, including but not limited to: full names, addresses, Social Security numbers, dates of birth, medical and treatment information, health insurance information, driver's license numbers, passport information, financial account information and contact information.

18. On information and belief, at the time of the Data Breach, MFHS failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the PII of approximately 461,070 current and former patients.[8]

19. Current and former patients of MFHS, such as Plaintiff and Class members, allowed their PII to be made available to MFHS with the reasonable expectation that MFHS would comply with its obligation to keep their sensitive and personal information, including their PII,

---

[6] *About Us*, Maternal & Family Health Services, https://www.mfhs.org/about-us/ (last accessed February 23, 2023).
[7] *Id.*
[8] *See Data Breach Notification*, Office of Maine Atty. General, https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml. (last visited February 22, 2023).

confidential and secure from illegal and unauthorized access, and that MFHS would provide them with prompt and accurate notice of any unauthorized access to their PII.

20. Unfortunately for Plaintiff and Class members, MFHS failed to carry out its duty to safeguard sensitive PII and provide adequate data security, thus failing to protect Plaintiff and Class members from the exfiltration of their PII during the Data Breach.

B. The Data Breach

21. MFHS disclosed in a Notice sent on or about January 3, 2023, to Plaintiff and other affected individuals that it was affected by a cyber-security incident described as a "ransomware incident" that occurred between "August 21, 2021 and April 4, 2022" where "elements of [patients'] personal information [] may have been compromised." *See* Notice of Data Breach, attached hereto as **Exhibit A**. Further, MFHS acknowledged that the unauthorized actor(s) was able to exfiltrate Plaintiff's and Class members' PII, "name, address, date of birth, social security number, driver's license number, financial account/payment card information, medical information and/or health insurance information." *Id.*

22. However, MFHS failed to disclose to Plaintiff and other victims of the Data Breach when the "unauthorized third party" first gained access to MFHS's systems and how long the unauthorized actor had access to Plaintiff's and Class members' information. Instead, MFHS admitted to the Office of the Maine Attorney General and various other state and federal governmental agencies that the unauthorized actor(s) had unfettered access to MFHS's computer systems, and Plaintiff's and other MFHS patients' PII, Social Security numbers, and other medical information, for almost **eight months**—between August 21, 2021 and April 4, 2022.[9]

[9] *See Data Breach Notification*, Office of Maine Atty. General, https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml. (last visited February 22, 2023).

23. MFHS asserts that upon discovering the Data Breach, it "reported the incident to law enforcement and worked with cybersecurity counsel and forensic experts to investigate how the incident occurred and what information was potentially compromised."[10]

24. Despite discovering the Data Breach on April 4, 2022, MFHS failed to determine that, during the eight months that the unauthorized actor had unfettered access to MFHS's computer systems, the unauthorized third party obtained and exfiltrated the PII, Social Security numbers, and medical records of MFHS's patients, such as Plaintiff and Class members, until much later.

25. Moreover, despite acquiring knowledge of the unauthorized access to its computer systems on April 4, 2022, and confirming that the unauthorized actors accessed and exfiltrated patient PII, Social Security numbers, and medical records, MFHS delayed sending individualized notice to affected patients until approximately January 3, 2023—**nine months** after discovery of the Data Breach.[11]

26. During the time that the unauthorized individuals had unrestricted access to MFHS's network, they were able to access and acquire personal, sensitive, and protected PII and medical information belonging to over tens of thousands of current and former MFHS patients.

C. MFHS's Many Failures Both Prior to and Following the Breach

27. MFHS could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and network files containing PII.

28. To be sure, collecting, maintaining, and protecting PII is vital to virtually every aspect of MFHS's operations as a medical treatment institute.

[10] *Id.*
[11] *Id.*

29. Despite such importance, MFHS failed to detect that its own data system was compromised for **eight months**, until on or around April 4, 2022.[12]

30. Moreover, when MFHS finally acknowledged that it had experienced a breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to Plaintiff's and Class members' PII, or even the full extent of the PII that was accessed during the Data Breach.

31. MFHS's failure to properly safeguard Plaintiff's and Class members' PII and medical information allowed the unauthorized actors to access this highly sensitive PII and medical information, and MFHS's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

32. MFHS acknowledged that it needs to "strengthen its system's security to prevent this kind of incident from happening again,"[13] impliedly admitting that its system was inadequate prior to the incident.

33. MFHS's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

34. First, MFHS failed to timely secure its computer systems to protect its current and former patients' PII and medical information. MFHS allowed the unauthorized actors to continue to have access to MFHS's systems for eight months, until MFHS finally discovered the Data Breach.

---

[12] *Id.*

[13] Healthnews, *Ransomware Attack Impacts Health Services Organization in Pennsylvania*, Ransomware Attack Impacts Health Services Organization in Pennsylvania | HealthNews (last visited February 2, 2023).

35. Second, MFHS failed to timely notify affected individuals, including Plaintiff and Class members, that their highly-sensitive PII had been accessed by unauthorized third parties. MFHS waited approximately nine months to provide notice to the victims of the Data Breach that their PII had been compromised.

36. Third, MFHS has made no effort to protect Plaintiff and the Class from the long-term consequences of MFHS's acts and omissions. Although the Notice offered victims a complimentary one-year membership to IDX credit monitoring services, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

37. In short, MFHS's myriad failures, including the failure to timely detect the Data Breach and to notify Plaintiff and Class members with reasonable timeliness that their personal and medical information had been exfiltrated due to MFHS's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII for months before MFHS finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

38. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

39. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed data.[14] Between January and July 2019,

[14] *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at

more than 31.6 million healthcare records were exposed in data security incidents—more than double the total amount of healthcare data breaches for all of 2018.[15]

40. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.[16] Conditions have only worsened since: Statista estimates that "[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]" and that "[i]n the first half of 2020, there were 540 reported data breaches."[17]

41. Data breaches are a constant threat because of the price that PII are sold for on the dark web. According to Experian, medical records sell on the dark web for prices that are hundreds or thousands of times the price of basic personal or financial information.[18] For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

42. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as

---

https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last accessed July 20, 2022).

[15] Steve Adler, *First Half of 2019 Sees 31.6 Million Healthcare Records Breached*, HIPAA Journal (Aug. 2, 2019), available at: https://www.hipaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached.

[16] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed (last accessed July 20, 2022).

[17] *Id.*

[18] *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, Experian (Dec. 6, 2017), available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

43. Data breaches involving medical and health information, like the one here at issue, amplify those risks considerably because of the access it provides to criminals.

44. When the PII includes medical information, the identity theft could extend to sending the victim fake medical bills or obtaining medical services using the victim's insurance or financial information, which can result in unknown, unpaid bills being sent to collections or using the victim's health insurance.[19]

45. Moreover, unlike victims of just credit card identity theft, victims of medical records data breaches cannot simply "reverse" fraudulent transactions.[20] As such, victims of data breaches in which hackers misappropriate highly sensitive patient PII often are unable to recover the losses they suffer as a result thereof, and must expend additional time and money to mitigate and protect themselves from further attempts at identity theft. One study found that the majority of medical identity theft victims had to pay an average of $13,500 to resolve issues stemming from

[19] Medical Identity Theft, Federal Trade Commission (Jan. 2011), available at: https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[20] *See The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction*, Accenture, available at: https://www.accenture.com/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf (last visited Feb. 12, 2021).

the data breach, and only 10% of victims achieve a completely satisfactorily resolution.[21] Almost one-third of medical identity theft victims lost their health insurance as a result of the identity theft.[22]

46. As explained by Kunal Rupani, director of product management at Accellion, a private cloud solutions company, in the context of a different medical data breach:

> Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. As a result, a patient's records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.[23]

47. SecureWorks, a division of Dell Inc., echoed that sentiment, noting that "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined."[24] The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."[25]

48. Similarly, the FBI Cyber Division in an April 8, 2014, Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims,

---

[21] *See Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC (Feb. 2015), at pp.2, 7, available at: https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.
[22] *Id.*
[23] Jeff Goldman, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach (Mar. 11, 2016), http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html (last visited Feb. 11, 2021).
[24] What's the Market Value of a Healthcare Record, Dell SecureWorks (Dec. 13, 2012), https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record (last visited Feb. 11, 2021).
[25] *Id.*

obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[26]

49. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing patient PII know the importance of protecting that information from unauthorized disclosure. Indeed, on information and belief, Defendant was aware of highly publicized security breaches where PII and protected health information was accessed by unauthorized cybercriminals, including breaches of computer systems involving: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[27]

50. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.

51. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

52. Further, consumers' PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen

[26] Federal Bureau of Investigation, FBI Cyber Division Private Industry Notification (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last visited Feb. 11, 2021).
[27] *See e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics (last accessed Feb. 15, 2021).

identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[28] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[29]

53. Social Security numbers are among the most dangerous kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]

54. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

---

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 20, 2022).

[29] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed July 20, 2022).

[30] Social Security Administration, *Identity Theft and Your Social Security Number*, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 20, 2022).

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

55. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

56. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[32]

57. Given the nature of MFHS's Data Breach, as well as the length of the time MFHS's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' PII can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

58. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[33] The

[31] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed July 20, 2022).
[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 20, 2022).
[33] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed July 20, 2022).

information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

59. To date, MFHS has offered its consumers *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they face for years to come, particularly in light of the PII at issue here.

60. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep PII private and secure, MFHS failed to take appropriate steps to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by MFHS's failure to implement or maintain adequate data security measures for its current and former patients.

E. MFHS Had a Duty and Obligation to Protect PII

61. MFHS has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. MFHS's obligations are derived from: 1) government regulations and state laws, including HIPAA and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII and medical records. Plaintiff and Class members provided, and MFHS obtained, their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

62. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII, regularly

review access to data bases containing protected information, and procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

63. Additionally, HIPAA requires Covered Entities and Business Associates to provide notification to every affected individual following the impermissible use or disclosures of any protected health information. The individual notice must be provided to affected individuals without unreasonable delay and no later than 60 days following discovery of the breach. Further, for a breach involving more than 500 individuals, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, *et seq.*

64. Defendant admits that it is subject to HIPAA.[34] As such, Defendant has an obligation to comply with HIPAA requirements concerning the protection of PII and protected health information and prompt and adequate notification of data breaches.

65. Additionally, the Federal Trade Commission's ("FTC") Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[34] *See Job Posting for Medical Office Assistant,* https://www.mfhs.org/careers/medical-office-assistant-scranton-pennsylvania-2/ (Job Duties include: "Ensures all consents, HIPAA and Disclosure of Information Template are completed in NextGen and confidentiality alerts are added as appropriate; ensure PHI log and Release of Records is completed, documented, and scanned into patient record.") (last visited February 22, 2023).

[35] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[36]

67. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[37]

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[38] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[39] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40] MFHS clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, and the amount of data exfiltrated.

---

[36] *Id.*
[37] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[38] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (Jan. 23, 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[39] *Id.*
[40] *Id.*

69. Here, at all relevant times, MFHS was fully aware of its obligation to protect the PII and protected health information of its current and former patients, including Plaintiff and the Class, and on information and belief, MFHS is a sophisticated and technologically savvy health center that relies extensively on technology systems and networks to maintain its practice, including transmitting its patients' PII, protected health information, and medical information in order to operate its business.

70. MFHS had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the PII and medical information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between MFHS and Plaintiff and Class members. MFHS alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' PII.

71. MFHS's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

72. Further, MFHS had a duty to promptly notify Plaintiff and the Class that their PII was accessed by unauthorized persons.

F. MFHS Violated HIPAA, FTC and Industry Standard Data Protection Protocols

73. HIPAA obligates Covered Entities and Business Associates to adopt administrative, physical, and technology safeguards to ensure the confidentially, integrity, and security of consumer and patient PII.

74. The FTC rules, regulations, and guidelines obligate businesses to protect PII, from unauthorized access or disclosure by unauthorized persons.

75. At all relevant times, Defendant was fully aware of its obligation to protect the customers and patient PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII, including personal health and medical records.

76. Defendant was also aware of the significant consequences of its failure to protect PII for the hundreds of thousands of patients who provided their PII and medical information to Defendant, and knew that this data, if hacked, would injure consumers, including Plaintiff and Class members.

77. Unfortunately, MFHS failed to comply with HIPAA, FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, MFHS failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of current and former patients' PII, including protected health and information and records that Defendant receives and maintains;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former patients' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former patients' PII.

78. Had MFHS implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. MFHS could have prevented or detected the Data Breach prior to the hackers accessing MFHS's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former patients of MFHS would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. MFHS's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

79. MFHS purports to care about data security and safeguarding patients' PII, and represents that it will keep secure and confidential the PII belonging to its current and former patients.

80. Plaintiff's and Class members' PII and medical information was provided to MFHS in reliance on its promises and self-imposed obligations to keep PII and medical information confidential, and to secure the PII and medical information from unauthorized access by malevolent actors. It failed to do so.

81. The length of the Data Breach also demonstrates that MFHS failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

82. Had MFHS undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as MFHS would have detected the Data Breach prior to the hackers extracting data from MFHS's

networks, and MFHS's current and former patients would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

83. Indeed, following the Data Breach, MFHS effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiff and others, MFHS acknowledged that the Data Breach required it to "take steps to strengthen its security posture to prevent similar event from occurring again in the future."[41]

H. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

84. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[42]

85. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[43]

86. The ramifications of MFHS's failure to properly secure PII, including Plaintiff's and Class members' PII, are severe. Identity theft occurs when someone uses another person's

[41] *See Data Breach Notification*, Office of Maine Atty. General, https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml. (last visited February 22, 2023).
[42] Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/. (last accessed July 20, 2022).
[43] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed July 20, 2022).

financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

87. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

88. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

89. Accordingly, MFHS's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[44] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[45] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[46] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

90. In response to the Data Breach, MFHS offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit monitoring. However, one year of

[44] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), available at http://www.iii.org/insuranceindustryblog/?p=267 (last accessed July 20, 2022).

[45] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), available at http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed July 20, 2022).

[46] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed July 20, 2022).

complimentary credit monitoring is a period much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by MFHS's failures.

91. Moreover, the credit monitoring offered by MFHS is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII.

92. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of PII, including protected health information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite MFHS's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

93. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and protected health information being accessed by cybercriminals, risks that will not abate within a mere one year: the unauthorized access of Plaintiff's and Class members' PII, especially their

Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that MFHS offered victims of the Breach. The one year of credit monitoring that MFHS offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

94. As a direct and proximate result of MFHS's acts and omissions in failing to protect and secure PII and medical information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

95. Plaintiff retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of herself and similarly situated individuals whose PII and medical information was accessed in the Data Breach.

96. MFHS is aware of the ongoing harm that the Data Breach has and will continue to impose on MFHS's current and former patients, as the notices that it posted and sent to Plaintiff and Class members regarding the Data Breach advise the victims to "remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information."[47]

I. Plaintiff Atkins's Experience

97. In January 2023, Plaintiff Atkins received a notice from Defendant that her PII had been improperly accessed and/or obtained by third parties. This notice indicated that Plaintiff Atkins's PII, inclusive of her name, address, telephone number, date of birth, Social Security

[47] *See Data Breach Notification*, Office of Maine Atty. General, https://apps.web.maine.gov/online/aeviewer/ME/40/aa8282f5-0293-41fe-8074-d62e568e05ac.shtml. (last visited February 22, 2023).

number, driver's license number, health insurance information, treatment information and/or health information, and financial information was compromised in the Data Breach.

98. As a result of the Data Breach, Plaintiff Atkins has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Atkins has spent several hours dealing with the Data Breach, valuable time Plaintiff Atkins otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

99. In December 2022, Plaintiff Atkins was forced to cancel one of her debit cards due to fraudulent activity in her bank account that, on information and belief, occurred as a result of the Data Breach.

100. As a result of the Data Breach, Plaintiff Atkins has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Atkins is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

101. Plaintiff Atkins suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Atkins; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

102. As a result of the Data Breach, Plaintiff Atkins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. As a result of the Data Breach, Plaintiff Atkins is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

103. Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose PII was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

104. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Pennsylvania whose PII was accessed in the Data Breach (the "Pennsylvania Subclass").

Excluded from the Pennsylvania Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

105. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of MFHS and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that approximately 461,070 individuals comprise the Class and were affected by the Data Breach. The members of the Class will be identifiable through information and records in MFHS's possession, custody, and control.

106. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over

the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether MFHS's data security and retention policies were unreasonable;

b. Whether MFHS failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether MFHS owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether MFHS breached any legal duties in connection with the Data Breach;

e. Whether MFHS's conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether MFHS breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of MFHS's conduct; and

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

107. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their PII compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of MFHS's uniform wrongful conduct.

108. Adequacy: Plaintiff is an adequate representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

109. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by MFHS's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, MFHS's records and databases.

110. MFHS has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I –- Negligence
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

111. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

112. This count is brought on behalf of all Class members.

113. MFHS owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that MFHS collected.

114. MFHS owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that MFHS collected.

115. MFHS owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

116. MFHS owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

117. MFHS solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

118. MFHS knew or should have known it inadequately safeguarded this information.

119. MFHS knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and Class members, and MFHS was therefore charged with a duty to adequately protect this critically sensitive information.

120. MFHS had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII and medical information was entrusted to MFHS on the understanding that adequate security precautions would be taken to protect the PII and medical information. Moreover, only MFHS had the ability to protect its systems and the PII stored on them from attack.

121. MFHS's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. MFHS's misconduct included failing to: (1) secure its systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

122. MFHS breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

123. MFHS breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

124. MFHS breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

125. The law further imposes an affirmative duty on MFHS to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

126. MFHS breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their PII had been improperly acquired or accessed.

127. MFHS breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about June 30, 2022.

128. As a direct and proximate result of MFHS's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

129. As a direct and proximate result of MFHS's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II –- Negligence *Per Se*
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

130. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

131. This count is brought on behalf of all Class members.

132. HIPAA obligates Covered Entities and Business Associates to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information." 45 CFR § 164.530(c).

133. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

134. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as MFHS, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of MFHS's duty.

135. The Pennsylvania Breach of Personal Information Notification Act ("BPINA"), 73 P.S. § 2301, *et seq.*, requires that entities in possession of PII belonging to Pennsylvania residents shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system without unreasonable delay. *See* 73 P.S. § 2303(a).

136. Furthermore, a violation of BPINA is deemed to be an unfair or deceptive act or practice in violation of the Pennsylvania Unfair Trade Practices & Consumer Protection Law ("UTPCPL"). 73 P.S. § 2308. The UTPCPL declares it unlawful for entities to employ "[u]nfair methods of competition and unfair or deceptive acts or practices . . ." *See* 73 P.S. § 201-3(a).

137. In addition to the FTC rules and regulations, the BPINA, and the UTPCPL, other states and jurisdictions where victims of the Data Breach are located require that MFHS protect PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

138. MFHS violated HIPAA, BPINA, the UTPCPL, and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards; and by unduly delaying reasonable notice of the actual breach. MFHS's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiff's and Class members' sensitive PII.

139. MFHS's violations of HIPAA, BPINA, the UTPCPL, Section 5 of the FTC Act and other applicable statutes, rules, and regulations constitutes negligence *per se*.

140. Plaintiff and the Class are within the category of persons HIPAA, BPINA, the UTPCPL, and the FTC Act were intended to protect.

141. The harm that occurred as a result of the Data Breach described herein is the type of harm HIPAA, BPINA, the UTPCPL, and FTC Act were intended to guard against.

142. As a direct and proximate result of MFHS's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in MFHS's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III –- Breach of Implied Contract
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

143. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

144. This count is brought on behalf of all Class members.

145. Plaintiff and the Class provided MFHS with their PII and medical information.

146. By providing their PII and medical information, and upon MFHS's acceptance of such information, Plaintiff and the Class, on one hand, and MFHS, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

147. The implied contracts between MFHS and Plaintiff and Class members obligated MFHS to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII and medical information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. MFHS expressly adopted and assented to these terms in its public statements, representations and promises as described above.

148. The implied contracts for data security also obligated MFHS to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII and medical information.

149. MFHS breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII and medical information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

150. As a direct and proximate result of MFHS's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII and medical information in MFHS's possession, and are entitled to damages in an amount to be proven at trial.

COUNT IV –- Bailment
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

151. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

152. This count is brought on behalf of all Class members.

153. Plaintiff's and Class members' PII was provided to MFHS.

154. In delivering their PII and, Plaintiff and Class members intended and understood that their PII would be adequately safeguarded and protected.

155. MFHS accepted Plaintiff's and Class members' PII.

156. By accepting possession of Plaintiff's and Class members' PII, MFHS understood that Plaintiff and the Class expected their PII to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

157. During the bailment (or deposit), MFHS owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their PII.

158. MFHS breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

159. MFHS further breached its duty to safeguard Plaintiff's and Class members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

160. MFHS failed to return, purge, or delete the PII belonging to Plaintiff and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

161. As a direct and proximate result of MFHS's breach of its duties, Plaintiff and the Class suffered consequential damages that were reasonably foreseeable to MFHS, including but not limited to the damages set forth herein.

162. As a direct and proximate result of MFHS's breach of its duty, Plaintiff's and Class members PII that was entrusted to MFHS during the bailment (or deposit) was damaged and its value diminished.

COUNT V –- Violation of the Pennsylvania Unfair Trade Practices & Consumer Protection Law
73 P.S. § 201-3, *et seq.*
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

163. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

164. This count is brought on behalf of the Pennsylvania Subclass.

165. The Unfair Trade Practices & Consumer Protection Law declares it unlawful for entities to employ "[u]nfair methods of competition and unfair or deceptive acts or practices . . ." *See* 73 P.S. § 201-3(a).

166. MFHS's deceptive and unfair acts, omissions, and conduct include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

167. MFHS had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' PII. This exclusive knowledge includes, but is not limited to, information that MFHS received through internal and other non-public audits and reviews that concluded that MFHS's security policies were substandard and deficient, and that Plaintiff's and Class members' PII and other MFHS data was vulnerable.

168. MFHS had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

169. MFHS also had exclusive knowledge about the length of time that it maintained individual's PII after they stopped using MFHS's services.

170. MFHS failed to disclose, and actively concealed, the material information it had regarding MFHS's deficient security policies and practices, and regarding the security of the sensitive PII and medical information. For example, even though MFHS has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, MFHS failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. MFHS also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former patients' PII and other records. Likewise, during the days and weeks following the Data Breach, MFHS failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

171. MFHS had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because

MFHS was in a fiduciary position by virtue of the fact that MFHS collected and maintained Plaintiff's and Class members' PII and medical information.

172. MFHS's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of MFHS's data security and its ability to protect the confidentiality of current and former patients' PII.

173. Had MFHS disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, MFHS would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, MFHS received, maintained, and compiled Plaintiff's and Class members' PII without advising that MFHS's data security practices were insufficient to maintain the safety and confidentiality of their PII.

174. Accordingly, Plaintiff and Class members acted reasonably in relying on MFHS's misrepresentations and omissions, the truth of which they could not have discovered.

175. MFHS's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the BPINA, UTPCPL, HIPAA and the FTC Act.

176. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should have reasonably avoided.

177. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of MFHS's deceptive acts and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to MFHS as their patients, and with the understanding that MFHS would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of MFHS and which is subject to further breaches so long as MFHS fails to undertake appropriate and adequate measures to protect data in its possession.

178. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring MFHS from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI – Violation of the Pennsylvania Unfair Trade Practices & Consumer Protection Law
Vis-à-Vis Violations of the Pennsylvania Breach of Personal Information Notification Act
(On behalf of Plaintiff and the Pennsylvania Subclass)

179. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

180. This count is brought on behalf of all Pennsylvania Subclass members.

181. A violation of the BPINA constitutes an unlawful practice in violation of UTPCPL. 73 P.S. § 2308.

182. Defendant, knowing and/or reasonably believing that Plaintiff's and Pennsylvania Subclass members' PII was acquired or accessed by unauthorized persons during the Data Breach, nevertheless failed to provide prompt, immediate, notice "without unreasonable delay," of the Data Breach to Plaintiff and the Pennsylvania Subclass as required by BPINA.

183. By violating BPINA, Defendant's conduct constitutes an unlawful practice in violation of the UTPCPL.

184. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VII –- Violation of State Data Breach Statutes
(By Plaintiff on behalf of the Class)

185. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

186. This count is brought on behalf of all Class members.

187. MFHS is a corporation that owns, maintains, and records PII, and computerized data including PII, about its current and former patients, including Plaintiff and Class members.

188. MFHS is in possession of PII belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

189. MFHS failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

190. MFHS, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members as required by following data breach statutes.

191. MFHS's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Illinois Statute 815 ILCS 530/1, *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

192. As a result of MFHS's failure to reasonably safeguard Plaintiff's and Class members' PII, and the failure to provide reasonable and timely notice of the Data Breach to

Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in MFHS's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VIII – Violation of State Consumer Protection Statutes
(On behalf of Plaintiff, the Class, and the Subclass)

193. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

194. This count is brought on behalf of all Class members.

195. MFHS is a "person" as defined in the relevant state consumer statutes.

196. MFHS engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiff and Class members. MFHS is engaged in, and its acts and omissions affect, trade and commerce. Further, MFHS's conduct implicates consumer protection concerns generally.

197. MFHS's acts, practices and omissions were done in the course of MFHS's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

198. MFHS's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and Class members that their PII was accessed by unauthorized persons in the Data Breach.

199. By engaging in such conduct and omissions of material facts, MFHS has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

200. MFHS's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of MFHS's data security and ability to protect the confidentiality of PII.

201. MFHS intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

202. Had MFHS disclosed that its data systems were not secure and, thus, vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, MFHS received, maintained,

and compiled Plaintiff's and Class members' PII without advising that MFHS's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the Class members acted reasonably in relying on MFHS's misrepresentations and omissions, the truth of which they could not have discovered.

203. Past breaches within the industry put MFHS on notice that its security and privacy protections were inadequate.

204. MFHS's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the BPINA,UTPCPL, and the FTC Act.

205. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

206. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of MFHS's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal and medical information entrusted to MFHS and with the understanding that MFHS would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of MFHS and which is subject to further breaches so long as MFHS fails to undertake appropriate and adequate measures to protect data in its possession.

207. MFHS's conduct described herein, including without limitation, MFHS's failure to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII, MFHS's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect Plaintiff's and Class members' PII, MFHS's failure to provide timely and accurate notice to of the material fact of the Data Breach, and MFHS's continued acceptance of Plaintiff's and Class members' PII constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq*.;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq.*;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq.*, and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq.*;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq*.;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

208. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring MFHS from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT IX –- Intrusion Upon Seclusion
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

209. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

210. This count is brought on behalf of all Class members.

211. Plaintiff bring this claim on behalf of persons who reside in Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

212. Plaintiff and Class members had a reasonable expectation of privacy in the PII that MFHS possessed and/or continues to possess.

213. By failing to keep Plaintiff's and Class members' PII safe, and by misusing and/or disclosing their PII to unauthorized parties for unauthorized use, MFHS invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

214. MFHS knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider MFHS's actions highly offensive.

215. MFHS invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

216. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their PII was unduly frustrated and thwarted. MFHS's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

217. In failing to protect Plaintiff's and Class members' PII, and in misusing and/or disclosing their PII, MFHS has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

COUNT X –- Unjust Enrichment
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

218. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

219. This count is brought on behalf of all Class members.

220. Plaintiff and the Class have an interest, both equitable and legal, in their PII and medical information that was collected and maintained by MFHS.

221. MFHS was benefitted by the conferral upon it of Plaintiff's and Class members' PII and by its ability to retain and use that information. MFHS understood that it was in fact so benefitted.

222. MFHS also understood and appreciated that Plaintiff's and Class members' PII and medical information was private and confidential and its value depended upon MFHS maintaining the privacy and confidentiality of that information.

223. But for MFHS's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provide or authorized their PII to be

provided to MFHS, and MFHS would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

224. As a result of MFHS's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that PII) MFHS has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

225. MFHS's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

226. Under the common law doctrine of unjust enrichment, it is inequitable for MFHS to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. MFHS's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

227. The benefit conferred upon, received, and enjoyed by MFHS was not conferred officiously or gratuitously, and it would be inequitable and unjust for MFHS to retain the benefit.

228. MFHS is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on MFHS as a result of its wrongful conduct, including specifically the value to MFHS of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits MFHS receives from the use and sale of that information.

COUNT XI –- Declaratory Judgment
(By Plaintiff on behalf of the Class, or, in the alternative, the Pennsylvania Subclass)

229. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

230. This count is brought on behalf of all Class members.

231. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

232. An actual controversy has arisen in the wake of the Data Breach regarding MFHS's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether MFHS is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that MFHS's data security measures remain inadequate.

233. Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

234. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that MFHS continues to owe a legal duty to secure Plaintiff's and Class

members' PII, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure PII.

235. The Court also should issue corresponding prospective injunctive relief requiring MFHS to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class members' PII.

236. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII in MFHS's possession, custody, and control is real, immediate, and substantial. If another breach of MFHS's network, systems, servers, or workstations occurs, Plaintiff and the Class will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

237. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to MFHS if an injunction is issued. Among other things, if another massive data breach occurs at MFHS, Plaintiff and the Class will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to MFHS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and MFHS has a pre-existing legal obligation to employ such measures.

238. Issuance of the requested injunction will serve the public interest by preventing another data breach at MFHS, thus eliminating additional injuries to Plaintiff and the thousands of Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in her favor and against MFHS, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representatives; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit MFHS from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the putative Class, demands a trial by jury on all issues so triable.

Date: February 24, 2023

Respectfully Submitted,

/s/ Bryan L. Clobes

Bryan L. Clobes
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
205 N. Monroe St.
Media, PA 19063
Telephone: (215) 864-2800
Facsimile: (312) 782-4485
bclobes@caffertyclobes.com

Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class